Upload Assignment: Assignment: Manipulating the Stack

ASSIGNMENT INFORMATION

Points Possible

10

We've covered how you can attack the call stack and make it do what you want. The example we covered in this module executed shellcode that we injected into the running process. For this assignment you're going to do something similar. The assignment has two parts.

In the first part, you need to write a program that has a buffer overflow flaw. This program also needs to have a third, uncalled function. So this gives us a total of at least three functions - **main(.)**, **smash(.)**, and **uncalled(.)**. DO NOT call the uncalled(.) function from your program!

In the second part, you need to create an exploit string that will force your program to execute the uncalled function (note, I didn't say call - you'll move the execution pointer to the code in this function). Don't use **printf(.)**; you'll be tempted to, but it buffers, and you'll be unable to clear the buffer prior to the program exiting. Use a different printing function.

Your printing function should print the term "sekkrit stuff!" prior to terminating/crashing.

You'll need to format this assignment so that when you turn it in, I can uncompress it and run it. You should compress your archive using TAR (i.e. tar -cvzf assignment.tgz assignment-directory). I've attached an example. I should be able to uncompress your submission, cd to the extracted assignment directory, execute run.sh, and see "sekkrit stuff!" printed to the terminal.

If I can't do this, I'll give you a zero on the assignment and you'll need to resubmit. Good luck! I've attached and example archive to get you started (see below disclaimer on program addresses).

Individual components are worth:

(25%) Flawed client program

(25%) You have formatted addresses and data correctly and are injecting into the program

(50%) You are able to exploit the program and print the secret.

DON'T PANIC! I may need to tweak addresses to get it to run on my system. That's okay. But I shouldn't need to tweak anything more than that.

assignment.tgz